REMARKS/ARGUMENTS

Favorable consideration of this application, as presently amended, and in light of the following discussion is respectfully requested.

Claims 1-11 are pending in the application. Claims 1-2 and 4-11 are amended by the present amendment. Support for the amended claims can be found in the original specification, claims and drawings.[1] No new matter is presented.

In the Final Office Action of January 31, 2006 (hereinafter, "Final Office Action", Claims 1, 2 and 4-11 were rejected under 35 U.S.C. § 102(e) as being anticipated by Ansell et al. (U.S. Patent No. 6,367,019, hereinafter, "Ansell"); and Claim 3 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Ansell, and further in view of Bernecker (U.S. Patent No. 5,435,599).

The Final Office Action asserts that Ansell teaches all the elements of independent Claims 1, 4-6 and 9-11. Applicants respectfully submit that amended independent Claims 1, 4-6 and 9-11 state novel features clearly not taught or rendered obvious by the applied references.

Amended independent Claim 1 relates to a transmitter device that transmits content to a receiver device by accessing a recording medium that stores both the content and management data that is changed based on usage of the content. The transmitter device comprises:

> storage means for storing a ***hash value*** calculated on the basis of the management data;
>
> communication means which, in authenticating of the receiver device, transmits the management data to the receiver device and ***receives a hash value calculated on the basis of the management data and a hash value calculated on the basis of management data changed based on the usage of the content from the receiver device***;

[1] e.g., specification, p. 11.

> determination means for determining whether the hash value of the management data received by the communication means matches the hash value of the management data stored in the storage means; and
>
> updater means for updating the hash value of the management data stored in the storage means to the hash value of the changed management data.

Claims 1, and 4-5 are directed to a transmitter; Claims 6 and 9-10 are directed to a receiver; and Claim 11 is directed to a system including both a transmitter and receiver for performing a cross authentication procedure, as discussed below.

A non-limiting exemplary embodiment of the cross authentication process is described, for example, at Fig. 5, and p. 10-12 and 17-19 of the specification. A computer (receiver) is connected to a DVD drive (transmitter) via a network. The computer performs a cross authentication with the DVD drive before supplying content data, such as sound or images (moving images or still images). In the cross-authentication process, the computer receives content management data describing the usage conditions related to the content data supplied by the DVD drive. The computer then updates the content management data in accordance with the usage of the content data by the computer (e.g., decrement a count value in response to the reproduction and copying of the content data).

The computer then determines hash values of the received content management data and the updated content management data by applying one-way hash function to each of the content management data received from the DVD drive and the updated content management data. The computer then sends the hash values of the received content management data and the updated content management data to the DVD drive. After the cross-authentication process with the DVD drive, the computer receives, from the DVD drive, the content data (encrypted), namely, data such as sound and images, and a content key that has encrypted the content data. The computer decrypts the content data with the content key, and reproduces the decrypted content data.

Hash values, also referred to as a message digest, are used for accessing data or for security, and is a number generated from a string of text (e.g., the management data, or the changed management data). The hash value is substantially smaller than the management data itself, and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value.

Turning to the applied reference, Ansell describes a system in which data, such as a musical track, is stored as a secure portable track (SPT) which can be bound to one or more specific external players and a particular storage medium.[2] The system restricts playback of the SPT to specific external players and ensures that playback is only from the original storage medium.[3] Ansell also describes that the SPT can be exchanged between authorized devices, such as a portable player (150) and external player (150B), by exchanging an encryption key, a random number, and signature.[4]

Ansell, however, fails to teach or suggest a transmitter device which stores a ***hash value*** calculated on the basis of management data, transmits management data to the receiver device and ***receives a hash value calculated on the basis of the management data and a hash value calculated on the basis of management data changed based on the usage of the content from the receiver device***, as recited in independent Claim 1.

In addressing the features of Claim 1, the Final Office Action relies on col. 9, line 58-col. 10, line 55 of Ansell. The cited portion of Ansell describes the process of exchanging the SPT between authorized devices such as the portable player (150) and the external player (150B), as described in the flow chart of Fig. 8. The portable player (150) initiates the exchange by sending a key exchange request message including a certificate corresponding to the portable player and a first random number. The external player (150B) responds by

[2] Ansell, col. 2, lines 6-10.
[3] Id., col. 2, lines 10-13.
[4] Id., Figs. 5, 8A-8B and col. 9, line 58-col. 10, line 55.

retrieving available keys and sending a reply message including the encrypted keys, the first random number, a second random number, and a certificate corresponding to the external player (150B). After the portable player (150) receives the reply message from the external player (150B) and performs authentication, it sends an exchange message including the encrypted keys, and the first and second random numbers. Thus, a series of exchanges of keys, random numbers and certificates is used to facilitate the exchange of data between the portable player and the external player.

However, none of the items exchanged between the portable player and the external player are related to ***a hash value calculated on the basis of management data changed based on the usage of the content from the receiver device***. Ansell fails to teach or suggest that a hash value is calculated based on the management data, whatsoever, much less that such data is stored and exchanged for authenticating the receiver device. Instead, the cited portion of Ansell only describes the exchange of keys, random numbers, and certificates that are associated with the devices themselves and not associated with management information. It should also be noted that the exchanged random numbers are just that, random numbers, and are not hash values calculated on the basis of management data or changed management data.

The Advisory Action of April 12, 2006, in maintaining the rejection set forth in the Final Office Action, states that Ansell "teaches there are restrictions placed on the external player" and "some of the restrictions include maximum number of time an SPT can be played..." and that "these restrictions constitute the management data which would be changed." However, as noted above, the restrictions described in Ansell are not used to form ***a hash value calculated on the basis of management data changed based on the usage of the content from the receiver device***, which is exchanged between the devices for authentication purposed, as recited in independent Claim 1.

Thus, Ansell fails to teach or suggest a transmitter device which stores a ***hash value*** calculated on the basis of management data, transmits management data to the receiver device and ***receives a hash value calculated on the basis of the management data and a hash value calculated on the basis of management data changed based on the usage of the content from the receiver device***, as recited in independent Claim 1.

Accordingly, Applicants respectfully request that the rejection of independent Claim 1 under 35 U.S.C. § 102(e) be withdrawn. For substantially similar reasons, Applicants submit that independent Claims 4-6 and 9-11 also patentably define over Ansell.

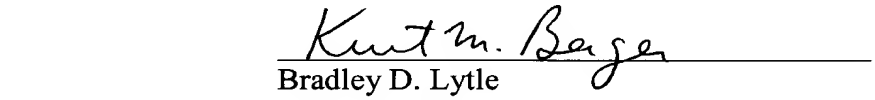
Claim 3 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Ansell in further view of Bernecker. As discussed above, Ansell fails to teach or suggest the above differentiated features recited in the pending independent claims. Likewise, Bernecker fails to remedy this deficiency, and therefore, none of the cited references, neither alone nor in combination teach or suggest Applicant's Claim 3, which includes the above distinguished features by virtue of dependency.

Accordingly, Applicants respectfully request that the rejection of Claim 3 under 35 U.S.C. § 103(a) be withdrawn.

Consequently, in view of the present amendment and in light of the foregoing comments, it is respectfully submitted that the invention defined by 1-11 is patentably distinguishing over the applied references. The present application is therefore believed to be in condition for formal allowance and an early and favorable reconsideration of the application is therefore requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.



Bradley D. Lytle
Attorney of Record
Registration No. 40,073
Andrew T. Harry
Registration No. 56,959

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 06/04)
GJM/ATH:aif

BDL/ATH/kkn
I:\ATTY\ATH\PROSECUTION\20'S\203772-US\203772 AM_070706.DOC

Kurt M. Berger, Ph.D.
Registration No. 51,461